

10/584,293
VQA 3/12/09

AMENDMENTS TO THE SPECIFICATION:

Please amend the caption on page 1, line 6, as follows:

BACKGROUND TO THE INVENTION
RELATED ART AND OTHER
CONSIDERATIONS

Please amend the caption on page 3, line 26, as follows:

BRIEF SUMMARY OF THE PRESENT INVENTION

Please amend the paragraphs beginning at page 3, line 27, and continuing to page 5, line 3, as follows:

In accordance with a first aspect of ~~the present invention~~ an example embodiment there is provided a method of authenticating a mobile node to a communication system, the communication system comprising a plurality of access nodes, the method comprising (a) generating a numerical chain comprising a series of values using a one-way coding function such that a given value within the chain is easily obtainable from a subsequent value, but the subsequent value is not easily obtainable from that given value; (b) sending a value from the first numerical chain from the mobile node to an access node to which the mobile node wishes to attach; and (c) using the sent value at the access node to authenticate the mobile node.

In accordance with a second aspect of ~~the present invention~~ an example embodiment there is provided a method of deriving a secure authentication key when a mobile node authenticates itself to an access node in accordance with any preceding claim, the method comprising providing a first authentication key K_{S0} for use by the mobile node and a first access node; sending a hash of the first authentication key $\text{hash}(K_{S0})$ to a second access node and the mobile node; and generating a new authentication key K_{S1} in accordance with the hash $\text{hash}(K_{S0})$.

10/584,293
A7 A3/12/09

In accordance with a further aspect of ~~the present invention~~ an example embodiment there is provided a mobile wireless terminal, the terminal comprising means for generating and storing a first numerical chain comprising a series of n values using a one-way coding function such that a given value within the chain is easily obtainable from a subsequent value, but the subsequent value is not easily obtainable from that given value; and means for disclosing values from the numerical chain to an access node in order to allow the access node to authenticate the mobile wireless terminal.

In accordance with a further aspect of ~~the present invention~~ an example embodiment there is provided an access node of a communication system having means for receiving from a mobile node a value of a first numerical chain comprising a series of n values using a one-way coding function such that a given value within the chain is easily obtainable from a subsequent value, but the subsequent value is not easily obtainable from that given value; and means for authenticating the mobile node on the basis of that value.

Please amend the paragraphs beginning at page 5, line 6, and continuing to page 5, line 9, as follows:

FIG. 2 illustrates diagrammatically the architecture of a communications network in accordance with an example embodiment ~~of the present invention~~; and

FIG. 3 is a flow diagram illustrating the method of certain example embodiments ~~of the present invention~~.

Please amend the paragraph beginning at page 5, line 11, and continuing through the remainder of page 5, as follows:

FIG. 2 illustrates diagrammatically the architecture of a cellular communications network for mobile wireless terminals in accordance with a first example embodiment ~~of the present invention~~, with like numerals representing like elements to those shown in FIG. 1. Access nodes 4, 6 are interconnected by a network. The network may be a